Paymentsite

Hosted Payments

User's Guide

For Hosted Payments Version 2.0

Last updated: April 27, 2011

Document version 2.0

Paymentsite Hosted Payments is created, owned, hosted, and managed by Maas Global Solutions

Paymentsite Hosted Payments User's Manual

Table of Contents

Paymentsite Hosted Payments User's Manual

Introduction to Paymentsite Hosted Payments

Paymentsite Hosted Payments from Maas Global Solutions is a hosted payment processing solution that allows merchants to collect payments from a web page without concerns about Payment Card Industry (PCI) security standards for collecting and storing sensitive customer information. Because the payments are processed on pages hosted by the MGS Level 1 PCI-certified secure payment gateway, merchant PCI requirements are greatly simplified. The solution is easily added to any web site with a simple HTML form. Some of the benefits of this solution are:

Ease of Use:

- HTML form post provides the easiest method to integrate with the Gateway
- To accept credit card and/or checks on a web page, all the merchant needs to do is get a gateway account and put a few lines of HTML code on their web page
- Settled funds are deposited directly into the merchant's bank account
    - Funds from all transaction types are generally available the next business day

Security:

- Data transmission happens using secure sockets layer (SSL) protocols to ensure confidential communications
- The Gateway submits a response to the merchant's web site to avoid data tempering attacks
- Merchants do not have to collect, transmit or store sensitive cardholder information to process transactions
    - There is no need for merchants to purchase and install a Secure Sockets Layer (SSL) digital certificate
    - This eliminates the complexity of securely handling and storing sensitive information, greatly simplifying compliance with the Payment Card Industry (PCI) Data Security Standard

Other Features:

- Full featured payment processing enables credit card authorizations, sales, and captures as well as electronic check payments
    - Since the Hosted Payments solution is intended for card-not-present transactions, returns, credits, and voids are not allowed through the posted interface, but are supported by logging into the merchant's back office
- Fraud protection measures (AVS, Card security code) are included
- Payment forms and receipts are customizable to match the merchant's web site
- Transactions flow as follows:
    - From the Merchant's web page
    - To a hosted payments page
    - To a hosted receipt page
    - Then back to the Merchant's web site

- Account on file allows the customer to save their card or checking account information so they don't need to re-enter each time they shop with a particular merchant
    - Repeat shoppers enjoy greater security since their sensitive information is not being transmitted each time they make a purchase
- A full-featured, intuitive Virtual Terminal and Back Office portal is included
    - The Virtual Terminal allows for processing in-person (and other) transactions, scheduling of recurring payments, and performing returns and credits
    - The Back office provides:
        - Customer information upload
        - Payment and receipt page customization
        - Comprehensive, real-time downloadable transaction reports
        - Unlimited users with user access management
        - Full suite of real-time transaction reporting

Transaction Types

The MGS Hosted Payments Solution allows for the following transaction types:

Authorization: If the merchant needs to make a credit or debit card sale, but won't be able to ship merchandise for several days; the merchant should use an authorization. An authorization transaction ensures the availability of fund and places a hold on those funds with the customer's bank, but does not transfer funds until a post-authorization or capture transaction is sent from the merchant. Once the goods are shipped, the merchant can capture the transaction to obtain the funds. This type of transaction is not sent for settlement until you submit a credit card post-authorization, or if the merchant marks the funds as shipped in the MGS Back Office reports.

Post-authorization: (a.k.a., post-auth or Capture) A post-authorization transaction sets a previous authorization transaction to capture the funds once the goods are shipped to the customer. The funds are then sent for settlement with the next batch. Merchants can perform a post-authorization transaction through the Hosted Payments interface—or they can use the Back Office to perform this function.

Sale: a credit or debit card Sale transaction is automatically submitted to the processor for both authorization and capture. If approved, the transaction will settle with the next batch settlement and funds will automatically be deposited in the merchant's bank account usually the next business day.

An electronic check sale transaction submits the information to the automated clearing house (ACH) network for funding.

Other transaction types such as returns, credits, and voids are supported but the merchant must log into the merchant back office and virtual terminal in order to perform these functions.

Submitting Transactions for Processing

To submit a transaction to the MGS Hosted Payments solution for processing, the merchant simply embeds HTML code into a web form and submits it to the Gateway. The customer filling out the form is then automatically transferred to the secure payment form on the MGS payment gateway.

Sample HTML code: Below is some sample HTML form code that shows the fields that might be submitted for a credit card sale. The merchant can choose which fields they wish to collect themselves and which they want the MGS Hosted Payments page to collect. If the merchant wishes to avoid the hassles associated with PCI standards, they should NOT collect any card or bank account information on their own servers.

```
<html>
<head>
<title>Merchant Web Form</title>
</head>
<body>
<h1>Merchant XYZ</h1>
<p>Customer Checkout</p>
<form method="post" action="https://<Hosted Payments Url>">
<input name="hp_merchant_id" type="hidden" value="123456" />
<input name="hp_txntype" type="hidden" value="sale" />
<input name="hp_amount" type="hidden" value="100.00" />
<input name="hp_method" type="hidden" value="ccard" />
<input name="hp_cardnum" type="hidden" value="4111111111111111" />
<input name="hp_expmonth" type="hidden" value="12" />
<input name="hp_expyear" type="hidden" value="2011" />
<input name="hp_bname" type="hidden" value="Joe Consumer" />
<input name="hp_baddr" type="hidden" value="123 Main St." />
<input name="hp_bcity" type="hidden" value="Moorpark" />
<input name="hp_bstate" type="hidden" value="CA" />
<input name="hp_bcountry" type="hidden" value="US" />
<input name="submit" type="submit" />
</form>
</body>
</html>
```

Setting up Hosted Payments

When the merchant signs up for a Hosted Payments account, they will receive a secure login for the MGS Virtual Terminal/Back Office.

To set up their hosted payments account, merchants must log into the Back Office, where they can configure the fields for their payment pages and several settings.

Merchants can opt to show or hide fields on their payment and receipt pages, so they have complete control over which information they collect themselves and which they wish the hosted pages to collect.

Additionally, merchants can configure the following settings in the Back Office. These settings must be provided before the merchant can begin using MGS Hosted Payments.

Setting	Function
Success URL	Customers will be redirected to this URL if the transaction is approved. The results of the transaction will be posted to this URL unless it is an html page.
Fail URL	Your customers will be redirected to this URL if the transaction fails to process successfully. The results of the transaction will also be posted to this URL unless it is an html page.
Submitted From	The domain where the request originated. This information is used to validate if the request came from the correct merchant's web site.
Success URL is Post	Indicates if the success URL can accept posted fields or not
Fail URL is Post	Indicates if the failure URL can accept posted fields or not
Show Billing Fields	Indicates whether billing fields will be displayed on the MGS hosted page
Show Shipping Fields	Indicates whether shipping fields will be displayed on the MGS hosted page
Show Payment Fields	Indicates whether payment fields will be displayed on the MGS hosted page
Show Result Page	Indicates whether our hosted transaction result page will be displayed to the customer

Input Field Definitions

The fields the merchant may pass to the MGS Hosted Payments Solution are shown in the table below.

Field name	**Possible values**/Description	Required?
hp_merchant_id	merchant account id	Required
hp_txntype	sale, auth, postauth	Configurable*
hp_amount	amount of transaction	Required
hp_method	ccard or echeck	Configurable*
hp_eciind	retail,moto,eci	Configurable*
hp_cardnum	credit or debit card number	Configurable*
hp_expmonth	2 digit card expiration month	Configurable*
hp_expyear	4 digit card expiration year	Configurable*

Field name	Possible values/Description	Required?
hp_cvv	3 or 4 digit card code printed on the card which is used for security measures to verify whether the customer has the card in their possession	Configurable*
hp_cvvind	If a CVV code is not able to be provided for a transaction, this field is available to identify why it is not provided. Possible values are: illegible, no_imprint, not_provided	Configurable*
hp_routingnumber	routing number, req for hp_method=echeck	Configurable*
hp_accountnumber	account number, req for hp_method=echeck	Configurable*
hp_bname	cardholderbilling name	Configurable*
hp_baddr	billing address	Configurable*
hp_baddr2	billing address 2	Configurable*
hp_bcity	billing city	Configurable*
hp_bstate	billing state, 2 characters	Configurable*
hp_bzip	billing zip	Configurable*
hp_bcountry	billing country	Configurable*
hp_phone	billing phone number	Configurable*
hp_email	billing email address	Configurable*
hp_sname	shipping name	Configurable*
hp_saddr	shipping address	Configurable*
hp_saddr2	shipping address 2	Configurable*
hp_scity	shipping city	Configurable*
hp_sstate	shipping state, 2 characters	Configurable*
hp_szip	shipping zip	Configurable*
hp_scountry	shipping country code, 2 characters	Configurable*
hp_refnum	merchant defined transaction identifier	Configurable*
hp_orderid	order id associated with this transaction, optional but the system will create a value if not passed by the merchant	Configurable*
hp_cf_1	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*
hp_cf_2	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*
hp_cf_3	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*
hp_cf_4	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*
hp_cf_5	Custom field for the merchant's use—will be passed back to the merchant in the response	Configurable*

* Fields shown here as configurable are the fields that the merchant may decide to show or hide on the MGS hosted pages. Some are required for a transaction to process, but are sensitive customer information protected by PCI standards, so if the merchant wishes to reduce PCI compliance hassles, we recommend the merchant chooses to show all sensitive required fields such as card number, account number, and CVV on the secure MGS hosted pages versus collecting those fields on their own web server.

Receipt Options

Merchants may choose to use the MGS Hosted Payment receipt pages or generate their own receipt pages using the response information passed back to the merchant web server after a transaction is processed.

To use the MGS hosted payment receipt page, the merchant must set the Show Result Page setting in the Back Office to "Yes".

If the merchant wishes to generate their own receipt page, they would set the Show Result Page to "No".

The merchant may host two separate results pages on their web server: one for approved transactions and one for failed (or declined) transactions. The merchant must identify both these URLs in the Settings section of the Back Office. Whether or not the merchant chooses to use the MGS hosted response pages, the merchant can still provide these two separate URLs for returning payees to their web site.

Response Fields

If the merchant indicates that their success and fail URLs can accept posted results, the MGS Hosted Payments solution will post back several fields to the merchant web server:

Field name	Description
hp_time	date and time of the transaction
hp_responsecode	response code, will be 0 if approved
hp_responsemsg	response message, APPROVED, DECLINED, or a relevant error message
hp_refnum	reference number passed in the request by the merchant
hp_transid	Hosted Payments system-defined transaction id
hp_avsresponse	avs response code
hp_cvvresponse	cvv response code
hp_authcode	process assigned authorization code
hp_orderid	either the system defined order id, or merchant assigned order id
hp_amount	transaction amount
hp_cf_1	Custom field for the merchant's use

hp_cf_2	Custom field for the merchant's use
hp_cf_3	Custom field for the merchant's use
hp_cf_4	Custom field for the merchant's use
hp_cf_5	Custom field for the merchant's use

Integrating and Testing a Merchant Implementation

To ensure successful payment processing, merchants should test their payment gateway integration carefully before attempting to process any real payment transactions.

To integrate and test an implementation:

1. Request a developer test account from MGS. MGS will provide the integration posting URL upon approval of your account, along with the URL and login credentials for the Back Office on the Integration Server.

2. Develop the web pages that will submit transactions to MGS Hosted Payments, containing the posting URL provided with your test account.

3. Log into the Back Office in the Integration Environment and set up your Hosted Payments configuration parameters.

4. Run a series of test transactions by submitting them through your web forms to the MGS Integration Environment. The Integration Environment mimics the live Payment Gateway, but does not submit transactions to any financial institutions, so no actual money will be passed.

5. You may log into your Back Office in the Integration Environment to view and download transaction reports from your test transactions. Note that test transactions will not settle.

6. Once you are satisfied that your implementation is working correctly, change the posting URL in your test web pages from the integration URL to the live posting URL. You will also need to log into the Production Back Office to choose your configuration settings—this information is not passed from Integration to the live system.

7. Confirm your production implementation by processing at least one live transaction from your web pages. Log into the Back Office system in Production and check your transaction reports to ensure the transaction is being passed to the live system rather than the Integration Server. Transactions run in production will transfer real money, so you may wish to test the live system using a small transaction amount (or void the transaction before it settles from your Back Office).

Fraud Protection: AVS and Card Code

The address verification system (AVS) and card code (CVV) are best practice fraud protection measures provided with the MGS Hosted Payments solution. If the merchant server accepts posted responses, whenever a transaction is processed by the MGS Hosted Payments system,

the system will pass back response AVS and CVV codes to help merchants determine whether or not they wish to accept the transaction.

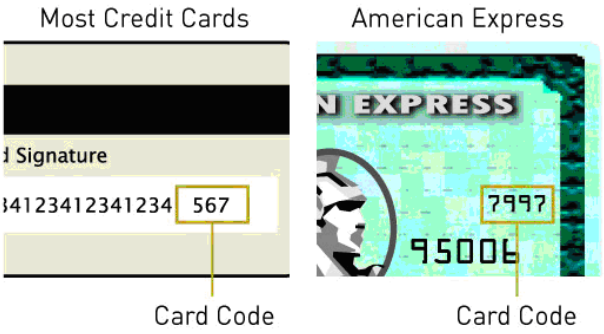
The AVS response is passed back to the merchant web server in the hp_avsresponse field. The values that are passed may be any of those shown in the table below.

Code	Alternates	Meaning
YYY	Y, YYA, YYD	Address: Match & 5 Digit Zip: Match
NYZ	Z	Address: No Match & 5 Digit Zip: Match
YNA	A, YNY	Address: Match & 5 Digit Zip: No Match
NNN	N, NN	Address: No Match & 5 Digit Zip: No Match
YYX	X	Address: Match & 9 Digit Zip: Match
NYW	W	Address: No Match & 9 Digit Zip: Match
XXW		Card Number Not On File
XXU		Address Information not verified for domestic transaction
XXR	R, U, E	Retry / System Unavailable
XXS	S	Service Not Supported
XXE		Address Verification Not Allowed For Card Type
XXG	G,C,I	Global Non-AVS participant
YYG	B, M	International Address: Match & Zip: Not Compatible
GGG	D	International Address: Match & Zip: Match
YGG	P	International Address: No Compatible & Zip: Match

Each of the digits in the AVS response have a meaning as well:

AVS CODE	DESCRIPTION
A	The street address matches, but the 5-digit ZIP code does not
B	Address information was not submitted in the transaction information, so AVS check could not be performed
E	The AVS data provided is invalid, or AVS is not allowed for the card type submitted
G	The credit card issuing bank is of non-U.S. origin and does not support AVS
N	Neither the street address nor the 5-digit ZIP code matches the address and ZIP code on file for the card
P	AVS is not applicable for this transaction
R	AVS was unavailable at the time the transaction was processed. Retry transaction
S	The U.S. card issuing bank does not support AVS
U	Address information is not available for the customer's credit card
W	The 9-digit ZIP code matches, but the street address does not match
Y	The street address and the first 5 digits of the ZIP code match perfectly

The Credit Card Verification Code, or Card Code, is a three- or four-digit security code that is printed on the back of credit cards (or on the front for American Express cards) as shown here:



A card code that is passed with a transaction from the MGS Hosted Payments system goes to the credit card issuer for verification. The credit card issuer determines if the value matches the value on file for the customer's credit card and returns a code indicating whether the code matched or not.

The card code (CVV, CVC, or CID) response gets passed back to the merchant's server in the hp_cvvresponse field. Possible values for the card code response and their meanings are shown in the table below.

CARD CODE RESPONSE	DESCRIPTION
N	The Card Code does not match
P	The Card Code was not processed
S	The Card Code was not indicated
U	Card Code is not supported by the card issuer